MEB:ADW
F. #2019R01108

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

UNITED STATES OF AMERICA

- against -

KENNETH UKHUEBOR and
PATIENCE OSAGIE,

Defendants.

- X

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH AND SEIZURE WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS 62-31 136TH STREET, FLOOR 2, QUEENS, NY 11367, INCLUDING ANY CLOSED CONTAINERS/ITEMS STORED THEREIN

- X

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST WARRANTS AND SEARCH AND SEIZURE WARRANT

Case No. 20-MJ-1155

EASTERN DISTRICT OF NEW YORK, SS:

ALEXANDER TURCZAK, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

Upon information and belief, in or about and between November 2018 and May 2020, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants KENNETH UKHUEBOR and PATIENCE OSAGIE, together with others, did knowingly and intentionally conspire to conduct one or more financial transactions in and affecting interstate and foreign commerce, which transactions involved the proceeds of

specified unlawful activity, to wit: bank fraud, bank fraud conspiracy, wire fraud and wire fraud conspiracy, in violation of Title 18, United States Code, Sections 1343, 1344 and 1349, knowing that the property involved in the transactions was to represent the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of the specified unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

Upon information and belief, there is probable cause to believe that there is kept and concealed within the premises known and described as 62-31 136th Street, Floor 2, Queens, New York 11367, the items described in Attachment B to this affidavit, all of which constitute evidence, fruits or instrumentalities of violations of 18 U.S.C. §§ 1343 (wire fraud), 1344 (bank fraud), 1349 (bank and wire fraud conspiracy) and 1956 (money laundering and money laundering conspiracy) (collectively, the "SUBJECT OFFENSES").

The source of your deponent's information and the grounds for his belief are as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since September 2017. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have participated in numerous investigations of violations of federal offenses including wire fraud, bank fraud and money laundering. I have also received training on the uses and capabilities of cellular telephones in connection with criminal activity.

2. This affidavit is made in support of an application for (i) warrants to arrest KENNETH UKHUEBOR and PATIENCE OSAGIE; and (ii) a warrant to search the premises located at 62-31 136th Street, Floor 2, Queens, New York 11367, as further described in Attachment A (the "SUBJECT PREMISES"), for the items to be seized described herein and in Attachment B.

3. The facts set forth in this affidavit are based upon my personal involvement in this investigation, my review of reports and other documents related to this investigation, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of the government's investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. Unless specifically indicated otherwise, all dates set forth below are on or about the dates indicated, and all amounts or sums are approximate.

THE SUBJECT PREMISES

4. The SUBJECT PREMISES is particularly described as the Second Floor of a multi-family residential home located at 62-31 136th Street, Queens, New York 11367. The home has two front door entrances. The entrance to the SUBJECT PREMISES is the left front door of the home, which has a small label affixed on the upper left corner with the word "2nd" written on it. A sign displaying the numbers "6231" is affixed to the brick exterior of the building, above and between the two front door entrances. A photograph of the building and the SUBJECT PREMISES is below and attached as part of Attachment A hereto.

PROBABLE CAUSE

Overview

5. As described in detail below, the defendants KENENTH UKHUEBOR and PATIENCE OSAGIE own and control several bank accounts that have received substantial sums of money from the victims of certain fraud schemes. The first scheme involved false promises to individuals that they would be entitled to large foreign inheritances upon payment of certain advance fees and charges. The second scheme involved fraudsters using hacked or false email accounts to deceive companies into diverting payments into certain bank accounts. The defendants controlled bank accounts that received proceeds from both of these fraud schemes. As described in this affidavit, the defendants received in these accounts at least $8 million in fraudulent proceeds.

The Defendants, Kenbor Inc. and Related Bank Accounts

6. Based on information and belief, the defendants KENNETH UKHUEBOR and PATIENCE OSAGIE are individuals both residing in Queens, New York.

7. Kenbor Inc. is a business corporation registered in New York State. Based on New York State Division of Corporations records, Kenbor Inc. was first registered in March 2015 and lists the defendant PATIENCE OSAGIE as the person who should receive any legal process on behalf of the company. As described below, Kenbor Inc. appears to be either the business operating name or the parent company of a clothing store operating as Kenbor Clothing. "Kenbor" appears to be a combination of "Kenneth" and "Ukhuebor."

8. On the business social networking website LinkedIn, a search for the name "Patience Osagie" yields several results. Only one of the results is for a user listed as residing in the New York area. The Patience Osagie residing in the New York area describes her work experience as being a boutique owner and fashion designer at Kenbor Inc. since January 2015. Notably, this account displays as a profile picture a heavyset adult male with a distinctive beard and wearing sunglasses. Based on my familiarity with the investigation to date, this appears to be the defendant KENNETH UKHUEBOR.

9. Through my investigation, I have identified two separate accounts on the social networking website Facebook, Inc. ("Facebook") that appear to belong to defendant KENNETH UKHUEBOR. The username for one of the accounts is "Kenneth Ukhuebor," and the username for the other account is "Ken Kenbor." Both accounts display profile pictures and other photographs depicting the same heavyset adult male shown in the profile picture for the aforementioned Patience Osagie LinkedIn account.

10. Defendant PATIENCE OSAGIE appears to have a Facebook account that displays the name "Precious Ukhuebor." The "Precious Ukhuebor" Facebook account displays profile photos and other pictures of OSAGIE and lists the user as "married." On February 14, 2020, the Precious Ukhuebor Facebook account posted a photo of OSAGIE with defendant KENNETH UKHUEBOR and included a Valentine's Day message. In addition, OSAGIE appears to have an account (username "ukhuebor_precious") on Instagram, a social networking site that allows users to post pictures with captions. OSAGIE's Instagram page includes numerous photos of defendant UKHUEBOR with accompanying descriptions that refer to him as her husband.

11. The URL for the Precious Ukhuebor Facebook account is www.facebook.com/patience.osagie.3958.

12. On the Precious Ukhuebor Facebook account, defendant PATIENCE OSAGIE describes her employment as "Kenbor Clothing," using a clickable link that leads to a "Kenbor Clothing" Facebook page. The page describes the business as a "Women's Clothing Store" and includes a post from October 16, 2019 announcing a grand opening. The Kenbor Clothing Facebook page displays the following image as its profile picture.

13. On October 16, 2019, defendant PATIENCE OSAGIE changed her Facebook profile picture to display the same Kenbor Clothing picture above. Also on October 16, 2019, both the Ken Kenbor and Precious Ukhuebor Facebook users posted links to the Kenbor Clothing Facebook page's grand opening announcement.

14. Records from Facebook reveal that both the Kenbor Clothing and the Ken Kenbor accounts were registered using the same phone number.

15. Based on the foregoing, I believe that defendants KENNETH UKHUEBOR and PATIENCE OSAGIE are married to each other, and that UKHUEBOR is affiliated with Kenbor Inc. through OSAGIE.

16. The defendants KENNETH UKHUEBOR and PATIENCE OSAGIE maintained at least three bank accounts to receive funds, and to launder those funds, related to the Advanced Fee Inheritance Scheme and the Business Email Compromise Scheme.

17. Bank records I have reviewed indicate that in or about April 2015, the defendant PATIENCE OSAGIE opened the bank account XXXXXXXXX8304 on behalf of Kenbor Inc. (the "8304 Account") at a federally-chartered bank, the deposits of which were insured by the Federal Deposit Insurance Corporation ("FDIC"), and which conducts business in New York and other states ("Bank #1").

18. Bank records I have reviewed indicate that in or about February 2019, defendant KENNETH UKHUEBOR opened the bank account XXXXXX4690 on his own behalf (the "4690 Account") at another federally-chartered bank, the deposits of which were insured by the FDIC, and which conducts business in New York and other states ("Bank #2").

19. Bank records I have reviewed indicate that in or about September 2019, defendant PATIENCE OSAGIE opened bank account XXXXX8113 on behalf of Kenbor Inc. (the "8113 Account"), which was maintained at Bank #2.

The Advanced Fee Inheritance Scheme

20. Based upon my training and experience, I am familiar with fraud schemes referred to as "advanced fee" schemes. A typical advanced fee inheritance scheme often involve fraudsters who target elderly victims by pretending to be the representatives of a foreign estate in which the victim has purportedly been named as a beneficiary of the estate and is entitled to a large sum of money. Such schemes sometimes involve promises by fraudsters that the victim will receive a large payment upon the victim's payment to the fraudsters of purported taxes, fees or other invented charges.

21. As part of the government's investigation, I interviewed an individual victim located in New York ("Victim #1") who sent $53,400 to Kenbor Inc. pursuant to the Advanced Fee Inheritance Scheme.[1] I also interviewed a personal assistant to Victim #1 (the "Assistant"), who provided me with copies of correspondence, faxes, and other documents relating to communications between Victim #1 and fraudsters. According to documents provided by the Assistant, a woman using the name "Catalina Moreno" (who held herself out as being a manager at a bank located in Spain) sent a letter to Victim #1 in November 2018, claiming that Victim #1 was entitled to a $26.7 million inheritance as long as Victim #1 first paid certain fees and charges. Victim #1 and Moreno then exchanged multiple messages via fax, with Moreno using a Spanish fax number. On or about December 18, 2018, Moreno sent Victim #1 a fax instructing him to write a check for $53,400 to Kenbor Inc. in connection with

[1] Victim #1 died in February 2020.

her claim that the payment to Kenbor Inc. would facilitate the release of millions of dollars in inheritance proceeds. That same day, Victim #1 wrote a check for $53,400 to Kenbor Inc. Later that day, an unknown individual deposited the $53,400 check into the 8304 Account, which, as described earlier, defendant PATIENCE OSAGIE opened on behalf of Kenbor Inc. Victim #1 later informed me that he did not recognize the names of defendant KENNETH UKHUEBOR or Kenbor Inc. and did not recall writing any checks to either UKHUEBOR or the company. Victim #1 never received any money or proceeds from Moreno or any other person or entity in connection with the purported inheritance.

22. I have also interviewed a second victim of the Advanced Fee Inheritance Scheme, an individual victim residing in Washington ("Victim #2"). According to Victim #2, in or about March 2019, he received a call from an individual using the name "Arne Zeidler," who held himself out as a London-based lawyer.[2] Zeidler purportedly informed Victim #2 that he was entitled to a $10.5 million inheritance held at a United Kingdom bank called Yorkshire Bank, contingent on Victim #2 first paying certain fees and charges. On or about July 17, 2019, Zeidler sent Victim #2 an email, instructing him to wire funds to the 4690 Account in connection with false promises that the payment would facilitate the release of millions of dollars in inheritance proceeds. As described above, defendant KENNETH UKHUEBOR had previously opened the 4690 Account in his own name. On or about July 18, 2019, Victim #2 wired $43,000 to the 4690 Account. Victim #2 never received any money or proceeds from Zeidler or any other person or entity in connection with the purported inheritance.

---

[2] Arne Zeidler appears to be an actual attorney based in London and founder of an international law practice called Zeidler Legal Services. The fraudster who communicated with Victim #2 appears to have impersonated the real Zeidler by creating and using the email address "azeidler@zeidlerlegalservice.com," whereas the real Zeidler's email address is "azeidler@zeidlerlegalservices.com."

The Business Email Compromise Scheme

23. Based upon my training and experience, I am familiar with fraud schemes referred to as "business email compromise" schemes. A business email compromise ("BEC") scheme often involves a computer hacker gaining unauthorized access to a business email account via software, malware or social engineering, blocking or redirecting communications to and/or from the email account, and then using the compromised email account or a separate fraudulent email account (sometimes called a "spoofed" email account)[3] to communicate with unsuspecting personnel from a victim company and trick them into making an unauthorized wire transfer. The fraudster directs the personnel to transmit company funds to the bank account of a third party (sometimes referred to as a "money mule"), which is often a bank account owned, controlled and/or used by individuals involved in the scheme. The money may then be laundered by transferring it through numerous bank accounts or by quickly withdrawing it as cash, by check or by cashier's check.

24. A publicly traded pharmaceutical company based in New Jersey and with offices in New York was a victim of a BEC scheme ("Company #1"). A pharmaceutical company based in New York ("Company #2") is a vendor for Company #1. As part of this investigation, I have interviewed representatives of Company #1 and received emails and other documents from them. According to those interviews and materials, in or about and between March 2020 and April 2020, Company #1 exchanged emails with an unknown fraudster that had

[3] One way of spoofing an email address is to create an account at a fraudulent domain, where the domain name is altered to appear identical to a real company domain but where it is misspelled by a letter or character. For example, a BEC fraudster might spoof the email address of "John" at "ACME, Inc." (john@acmecompany.com) by creating similar email accounts at a fraudulent domain (e.g., john@acmecornpany.com, replacing the "m" in "company" with the letters "rn," or john@acmecompanies.com). Also, BEC fraudsters sometimes create a fraudulent email account at a legitimate email provider (e.g., john_acmecompany@gmail.com).

gained unauthorized access to and was using the e-mail address of an employee of Company #2. On or about April 7, 2020, the person who had gained unauthorized access to the Company #2 account emailed a purportedly voided check to Company #1 in connection with requests to send future payments to the 8113 Account. As described earlier, defendant PATIENCE OSAGIE opened the 8113 Account in September 2019 on behalf of Kenbor Inc. In or about April 2020 and May 2020, Company #1 wired more than $8,000,000 to the 8113 Account. Company #1 subsequently discovered the fraud and ceased making payments to the 8113 Account.

The Defendants' Money Laundering

25. After receiving proceeds of the Advance Fee Inheritance and Business Email Compromise schemes described above into bank accounts controlled by them, the defendants KENNETH UKHEUBOR and PATIENCE OSAGIE, together with others, withdrew cash, purchased checks, sent wire transfers, wrote checks, charged debit cards and used other methods of disposing of the proceeds to conceal and disguise the nature, location, source, ownership and control of the proceeds.

26. As described in paragraph 21, Victim #1 wrote a check for $53,400 to Kenbor Inc. on or about December 18, 2018, and an unknown individual deposited the check into the 8304 Account on the same day. On or about December 19, 2018, an unknown individual withdrew $30,000 in cash from the 8304 Account. And on or about December 20, 2018, an unknown individual withdrew $15,000 in cash from the 8304 Account.

27. As described in paragraph 22, Victim #2 wired $43,000 to the 4690 Account on or about July 18, 2019. On or about July 19, 2019, an unknown individual withdrew $8,500 in cash from the 4690 Account. On or about July 22, 2019, an unknown individual withdrew $29,980 in cash from the 4690 Account. And on or about July 24, 2019, an

unknown individual withdrew $4,000 in cash from the 4690 Account and wired $700 to another bank account.

28. As described in paragraph 24, Company #1 wired more than $8,000,000 to the 8113 Account between April 2020 and May 2020. During that same period of time, one or more unknown individuals withdrew cash from, wrote checks out of and charged debit cards to the 8113 Account in amounts totaling more than $1,000,000. More than $900,000 of the proceeds successfully drawn on the 8113 Account during this period were written out as checks. The signatures on all of those checks appear to be similar and consistent with the same signature of defendant PATIENCE OSAGIE used to open the 8113 Account.

The Defendants' Use of the Subject Premises

29. Records obtained from Bank #1 show that when defendant PATIENCE OSAGIE opened the 8304 Account, she provided the address of the SUBJECT PREMISES. In addition, bank statements for the 8304 Account list the address of the SUBJECT PREMISES

30. Records obtained from Bank #2 show that when defendant PATIENCE OSAGIE opened the 8113 Account, she provided the address of the SUBJECT PREMISES. In addition, bank statements for the 8113 Account list the address of the SUBJECT PREMISES.

31. On May 15, 2020, the Honorable Robert M. Levy issued a warrant authorizing the search and seizure of certain historical location information for a cell phone believed to be used by defendant KENNETH UKHUEBOR. See Case No. 20-MC-1088. Information searched and seized pursuant to that warrant shows that UKHUEBOR's pattern of movement is consistent with his residing at the SUBJECT PREMISES.

32. On June 5, 2020, the Honorable Steven M. Gold issued a warrant authorizing the search and seizure of certain prospective GPS location information for the same

cell phone that was the subject of the 20-MC-1088 application. See Case No. 20-MC-1279. Information searched and seized pursuant to that warrant shows that defendant KENNETH UKHUEBOR's pattern of movement is consistent with his residing at the SUBJECT PREMISES.

33. On November 30, 2020, law enforcement surveilled the SUBJECT PREMISES. At approximately 6:45 a.m. that day, agents observed two vehicles parked near the SUBJECT PREMISES, including a black Toyota 4Runner with Pennsylvania license number KRK7348. At approximately 9:50 a.m. that day, agents observed the defendant KENNETH UKHUEBOR exit the SUBJECT PREMISES, enter the Toyota 4Runner and drive away.

34. Based on the foregoing, I believe that the defendants KENNETH UKHUEBOR and PATIENCE OSAGIE regularly reside at the SUBJECT PREMISES. Therefore, it is likely that any electronic devices that the defendants possess, including any that have used in connection with or in furtherance of the SUBJECT OFFENSES, will also be in the SUBJECT PREMISES.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

35. Based on my training and experience, I know that individuals who engage in wire fraud, bank fraud and money laundering activities commonly use phones, computers, or other electronic devices[4] to access websites used for illegal activity, to communicate with

[4] These electronic devices may include, but are not limited to, any computer, computer system and high-speed data processing device, including, but not limited to, desktop computers, notebook computers, tablets, and server computers; mobile phones, including, but not limited to, smart phones capable of transmitting electronic messages (such as text messages and email messages); computer disks; disk drives; any electronic data storage devices including, but not limited to, hardware, software, diskettes, CD-ROMs, DVDs, RAM, flash memory devices, and other storage mediums; and any input/output peripheral devices, including, but not limited to, data security devices.

victims and co-conspirators online, and to store records relating to transactions conducted as part of their illegal activities. As a result, they often store data on their computers related to their illegal activity, which can include logs of online chats with co-conspirators; electronic communications with victims; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts; and electronic records of financial transactions.

36. Based on my training and experience, I also know that when phones, computers, or other electronic devices are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

a. Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

b. Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.

c. In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, optical media, or portable hard drives.

37. In addition to there being probable cause to believe that phones and/or computer devices will be found on the SUBJECT PREMISES that contain evidence of the SUBJECT OFFENSES, there is also probable cause to believe that these devices constitute instrumentalities and/or contraband subject to seizure, in that the devices were used to commit the SUBJECT OFFENSES.

38. Based on the foregoing, I respectfully submit there is probable cause to believe that defendants KENNETH UKHUEBOR and PATIENCE OSAGIE engaged in the SUBJECT OFFENSES, and that evidence of this criminal activity is likely to be found in the SUBJECT PREMISES and in the closed containers/items stored therein, including any electronic devices found on the defendants' persons while they are physically present in the SUBJECT PREMISES.

A. Procedures for Searching ESI

Execution of Warrant for ESI

39. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information," including for "later review." Consistent with Rule 41, this application requests authorization to seize the items listed in Attachment B and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

a. First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.

b. Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

c. Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.

d. Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

Review of ESI

40. Following seizure of any electronic devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the Government, attorney support staff, agency personnel assisting the Government in this investigation, and outside technical experts under Government control) will review the ESI contained therein for information responsive to the warrant.

41. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the SUBJECT OFFENSES. Such techniques may include, for example:

a. surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

b. conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);

c. "scanning" storage areas to discover and possibly recover recently deleted data or deliberately hidden files;

d. performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation;[5] and

e. reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

42. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review

[5] Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches only work for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

Return of ESI

43. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the SUBJECT OFFENSES.

B. Biometric Unlocking

44. In my training and experience, it is likely that if the defendants KENNETH UKHUEBOR or PATIENCE OSAGIE has any electronic devices on their persons or in their belongings, then one or more of those devices uses biometric unlocking features, such as facial recognition unlocking.

45. The warrant I am applying for would permit law enforcement to compel the defendants KENNETH UKHUEBOR and PATIENCE OSAGIE to unlock any electronic devices using the devices' biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and

iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain cellular phone devices. In order to activate this unlocking mechanism, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the

infrared-sensitive camera detects the registered irises. Iris recognition features on other manufacturers' devices have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. I also know from my training and experience, as well as from information found in publicly available materials, including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked, or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Biometric features from other electronic device brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. The passcode or password that would unlock a given device recovered during execution of the requested warrant likely will not be known to law enforcement. Thus, in attempting to unlock any such devices for the purpose of executing the

search authorized by the requested warrant, it will likely be necessary to press the finger(s) of the user on the fingerprint reader of any device capable of biometric unlocking. The government may not otherwise be able to access the data contained on the electronic devices for the purpose of executing the search authorized by this warrant.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device.

46. Due to the foregoing, if any of the defendants KENNETH UKHUEBOR's or PATIENCE OSAGIE's electronic devices may be unlocked using one of the aforementioned biometric features, then the warrant I am applying for would permit law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of the relevant defendant against the fingerprint scanner of the device; (2) hold the relevant defendant in place while holding the device in front of his or her face to activate the facial recognition feature; and/or (3) hold the relevant defendant in place while holding the device in front of his or her face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

47. Law enforcement officers will select which fingers to press to the relevant defendant's electronic devices. The warrant does not authorize law enforcement to compel that either defendant KENNETH UKHUEBOR or PATIENCE OSAGIE state or otherwise provide the password or any other means that may be used to unlock or access any electronic devices. Moreover, the warrant does not authorize law enforcement to compel the defendants to identify the specific biometric characteristics (including unique fingerprint(s) or other physical features) that may be used to unlock or access any electronic devices.

REQUEST TO SEAL

48. I respectfully request the Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, and any arrest and/or search warrants. The investigation currently being conducted is ongoing. This affidavit sets forth significant information concerning the investigation, including information about the targets of the investigation and the matters being investigated. Premature disclosure of such information could jeopardize the continuing investigative activities including the execution of the warrants and could result in the destruction of evidence or the flight of individuals to avoid prosecution.

CONCLUSION

49. For all the reasons described above, there is probable cause to arrest KENNETH UKHUEBOR and PATIENCE OSAGIE, and probable cause believe that evidence of the SUBJECT OFFENSES, as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT PREMISES, as further described above and in Attachment A of this affidavit.

WHEREFORE, your affiant respectfully requests that (1) the Court issue warrants to arrest defendants KENNETH UKHUEBOR and PATIENCE OSAGIE so that they may be dealt with according to law; (2) the Court issue a warrant to search the premises known and described as 62-31 136th Street, Floor 2, Queens, New York 11367, as described herein and in Attachment A hereto, and to seize the items and information as specified in Attachment B to this affidavit and to the proposed search warrant.

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and warrants, be sealed until further order of the Court.

ALEXANDER TURCZAK
Special Agent
Federal Bureau of Investigation

Sworn to before me this
3d day of December, 2020

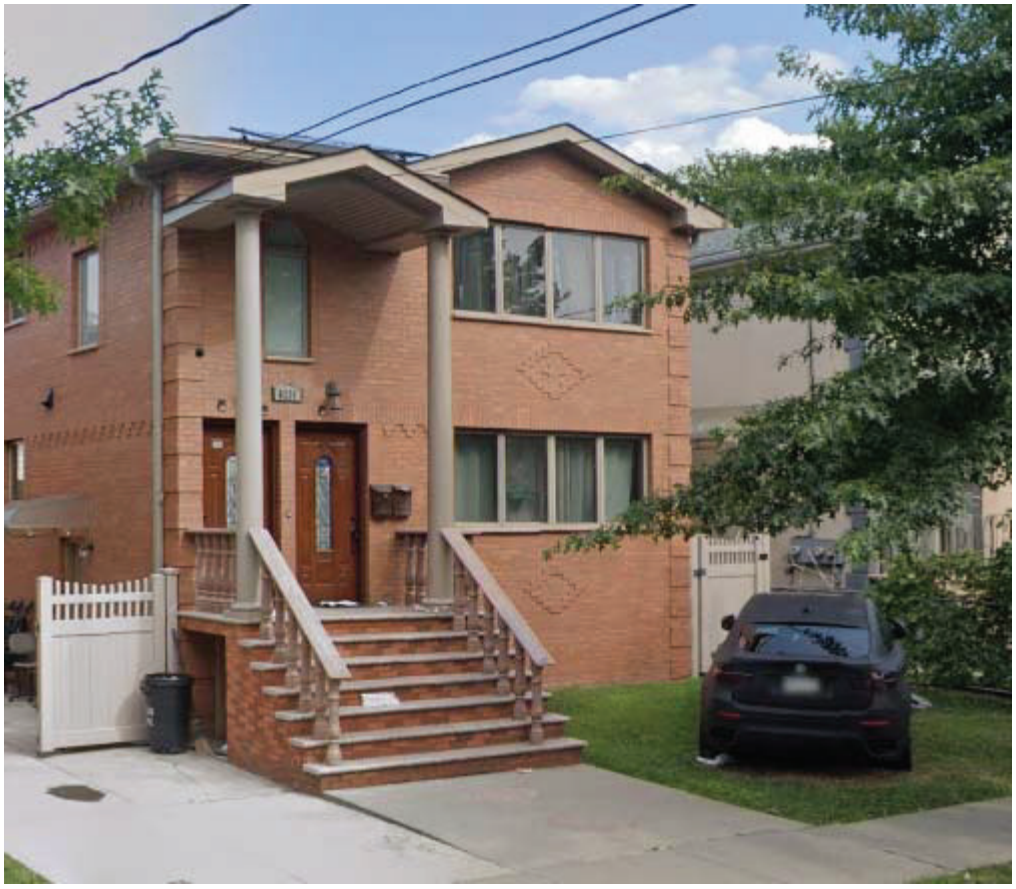
SWORN TELEPHONICALLY

[redacted]
THE HONORABLE SANKET J. BULSARA
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

PROPERTY TO BE SEARCHED

The premises to be searched (the "SUBJECT PREMISES") is particularly described as the Second Floor of a multi-family residential home located at 62-31 136th Street, Queens, New York 11367. The home has two front door entrances. The entrance to the SUBJECT PREMISES is the left front door of the home, which has a small label affixed on the upper left corner with the word "2nd" written on it. A sign displaying the numbers "6231" is affixed to the brick exterior of the building, above and between the two front door entrances. A photograph of the building and the SUBJECT PREMISES is below.



ATTACHMENT B

PROPERTY TO BE SEIZED

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), 1344 (bank fraud), 1349 (bank and wire fraud conspiracy) and 1956 (money laundering and money laundering conspiracy) (collectively, the "SUBJECT OFFENSES"), for the time period from November 1, 2018 to present, namely:

a. Books, records, receipts, notes, ledgers and other papers relating to the SUBJECT OFFENSES;

b. Proceeds of the SUBJECT OFFENSES, including United States currency, precious metals, jewelry, and financial instruments, including certificates of deposit and stocks and bonds;

c. Address and/or telephone books, rolodex indices, and any pagers or cell phones that have the ability to store names, addresses, telephone numbers, pager numbers, fax numbers of co-conspirators, information regarding financial institutions, and other individuals or businesses with whom a wire fraud conspiracy, bank fraud conspiracy, or money laundering relationship exists;

d. Documents and articles of personal property relating to the identity of the persons occupying, possessing, residing in, owning, frequenting or controlling the SUBJECT PREMISES to be searched or property therein, including rental agreements and records, property acquisition records, utility and telephone bills and receipts, photographs, answering machine tape recordings, cellular telephones, storage records, vehicle records, cancelled mail envelopes, correspondence, bank records, safety deposit box records, cancelled checks and other records of income and expenditure, credit card and bank records, travel documents and personal identification documents; and

e. Any phones, computers, or other electronic devices that reasonably appear to contain evidence of the above items or to be instrumentalities and/or contraband because they were used to commit the SUBJECT OFFENSES.[1]

f. Evidence of user attribution showing who used or owned any phones, computers, or other electronic devices seized from the SUBJECT PREMISES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history

The term "electronic devices" may include, but are not limited to, any computer, computer system and high-speed data processing device, including, but not limited to, desktop computers, notebook computers, tablets, and server computers; mobile phones, including, but not limited to, smart phones capable of transmitting electronic messages (such as text messages and email messages); computer disks; disk drives; any electronic data storage devices including, but not limited to, hardware, software, diskettes, CD-ROMs, DVDs, RAM, flash memory devices, and other storage mediums; and any input/output peripheral devices, including, but not limited to, data security devices

The passcode or password that would unlock and access any phones, computers or electronic devices seized from the SUBJECT PREMISES is not known to law enforcement. If it appears that any such device can be enabled with a "Touch ID," "Trusted Face" or any similar biometric feature (the "SUBJECT DEVICE"), and to the extent either defendant KENNETH UKHUEBOR or PATIENCE OSAGIE reasonably appears to be a user of any such SUBJECT DEVICE, law enforcement will be authorized to (1) press or swipe the fingers (including thumbs) of the relevant defendant to the fingerprint scanner of the SUBJECT DEVICE; (2) hold the SUBJECT DEVICE in front of the face of the relevant defendant to activate the facial recognition feature; and/or (3) hold the SUBJECT DEVICE in front of the face of the relevant defendant and activate the iris scanning recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this search warrant.

---

[1] For the avoidance of doubt, the items to be seized do not include any phones, computers, or other electronic devices that reasonably appear to be within the exclusive possession or control of any individuals other than KENNETH UKHUEBOR and PATIENCE OSAGIE.